The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
11/08/2016

SUBJECT:
Multiple Vulnerabilities in Microsoft Windows Could Allow Remote Code Execution (MS16-130)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Windows, the most severe of which could allow for remote code execution. The most severe vulnerability is triggered if a user opens a specially crafted image file. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:
- Windows Vista, 7, 8.1, RT 8.1, 10
- Windows Server 2008, 2008 R2 (including Server Core installations)
- Windows Server 2012, 2012 R2 (including Server Core installations)
- Windows Server 2016 (including Server Core installations)

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Microsoft Windows that could allow arbitrary code execution. The most severe vulnerability is triggered if a user opens a specially crafted image file. An attacker could exploit this vulnerability by convincing a user to visit a webpage or open an email in order to open a specially crafted, malformed image file. Details of these vulnerabilities are as follows:

- One remote code execution vulnerability exists when Windows image file loading functionality does not properly handle malformed image files. (CVE-2016-7212)
- One elevation of privilege vulnerability exists in the Windows Task Scheduler. (CVE-2016-7221)
- One elevation of privilege vulnerability exists in the Windows Input Method Editor (IME). (CVE-2016-7222)

Successful exploitation of this vulnerability could result in the attacker running arbitrary code and gaining the same rights as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Microsoft:

https://technet.microsoft.com/en-us/library/security/ms16-130.aspx

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7212
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7221
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7222